Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Digital Service Providers and the NIS-Directive

Consequences and impact

Huub Janssen

Chairman NIS CA DSP’s

September 19, 2019

Topics

1. NIS Directive
2. Who is a DSP?
3. Consequences?

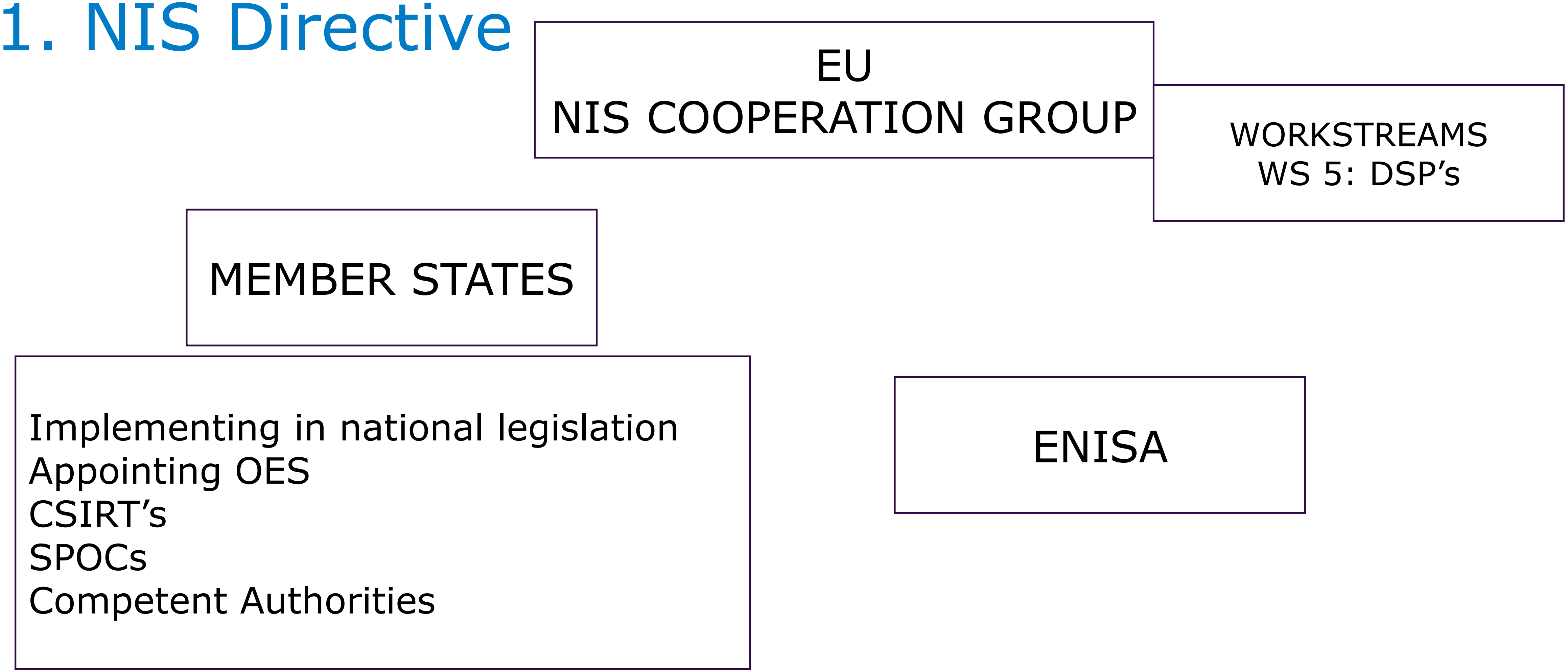
NIS Directive

1. Purpose
2. Issues
3. OES
4. DSP

1. NIS Directive

- Purpose NIS Directive
  - Network and Information Systems crucial for society
  - Incidents are increasing (amount, impact, complexity)
  - Incidents could cause major effect on EU economy
  - Focus
    - Operator of Essential Services (OES)
    - Digital Service Providers (DSP)
  - OES/DSP's should ensure the security of the network and information systems
  - Need for risk assessment and implementation of security measurements
  - Measurements should be proportionate to the risk presented

1. NIS Directive



EU
NIS COOPERATION GROUP

WORKSTREAMS
WS 5: DSP’s

MEMBER STATES

Implementing in national legislation
Appointing OES
CSIRT’s
SPOCs
Competent Authorities

ENISA

2. Issues

‘security of network and information systems’ means:

- the ability of network and information systems to
- resist, at a given level of confidence, any action that compromises
- the availability, authenticity, integrity or confidentiality
- of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems

3. Operators of Essential Services

- Appointed by Member States
- In following sectors:
  - Energy
  - Transport
  - Banking
  - Financial market infrastructures
  - Health sector
  - Drinking water
  - Digital infrastructure
- National supervision and regulation

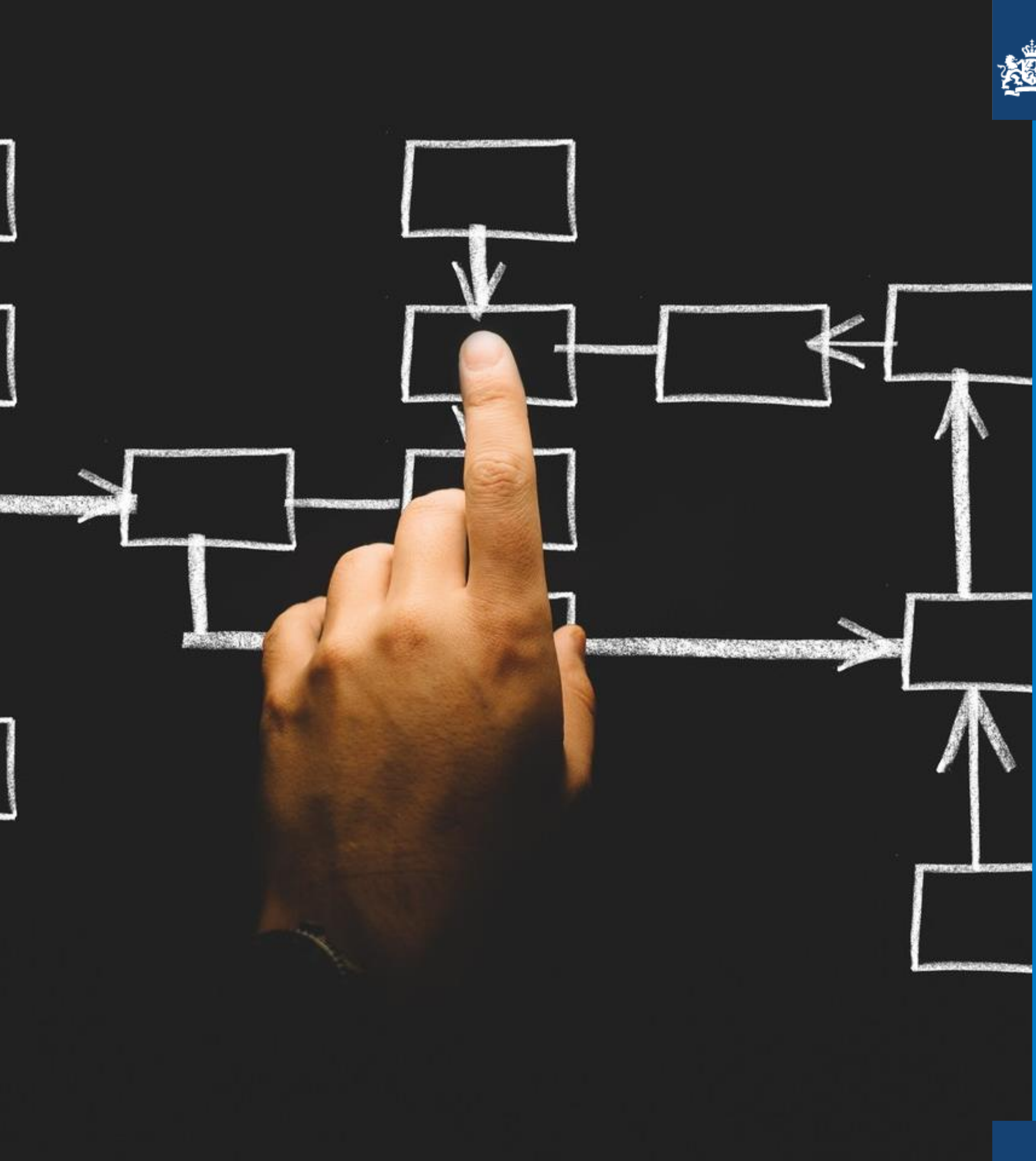
4. Digital Service Providers (DSP’s)

- DSP by definition
- Three types of DSP’s:

Online marketplace

Cloudcomputing services

Online Search engine



Who is DSP?

1. Online marketplace
2. Online search engine
3. Cloud service provider
4. SME exception

1. Online Marketplace

- allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts.
- B2C and B2B
- Characteristics:
  - Direct online sales of services and goods
  - Three parties involved
  - No intermediate sites or services
  - Processes (personal) data, transactions

Examples market places

Business to Consumer	Business to Business
Retail-platforms	Food and flower auctions
Sharing economy	Financial and insurance platforms (fintech)
Software/app shops	Advertising and profiling
Medicine	Commodity trading (e.g. oil, gas, electricity)
Cryptocurrency brokers	Resourcing, recruitment, staffing (employees)
Travel/holiday websites	
(Food) delivery services	
Sexual services	
Darkweb platform	

2. Online search engine

- allows the user to perform searches of, in principle, all websites on the basis of a query on any subject

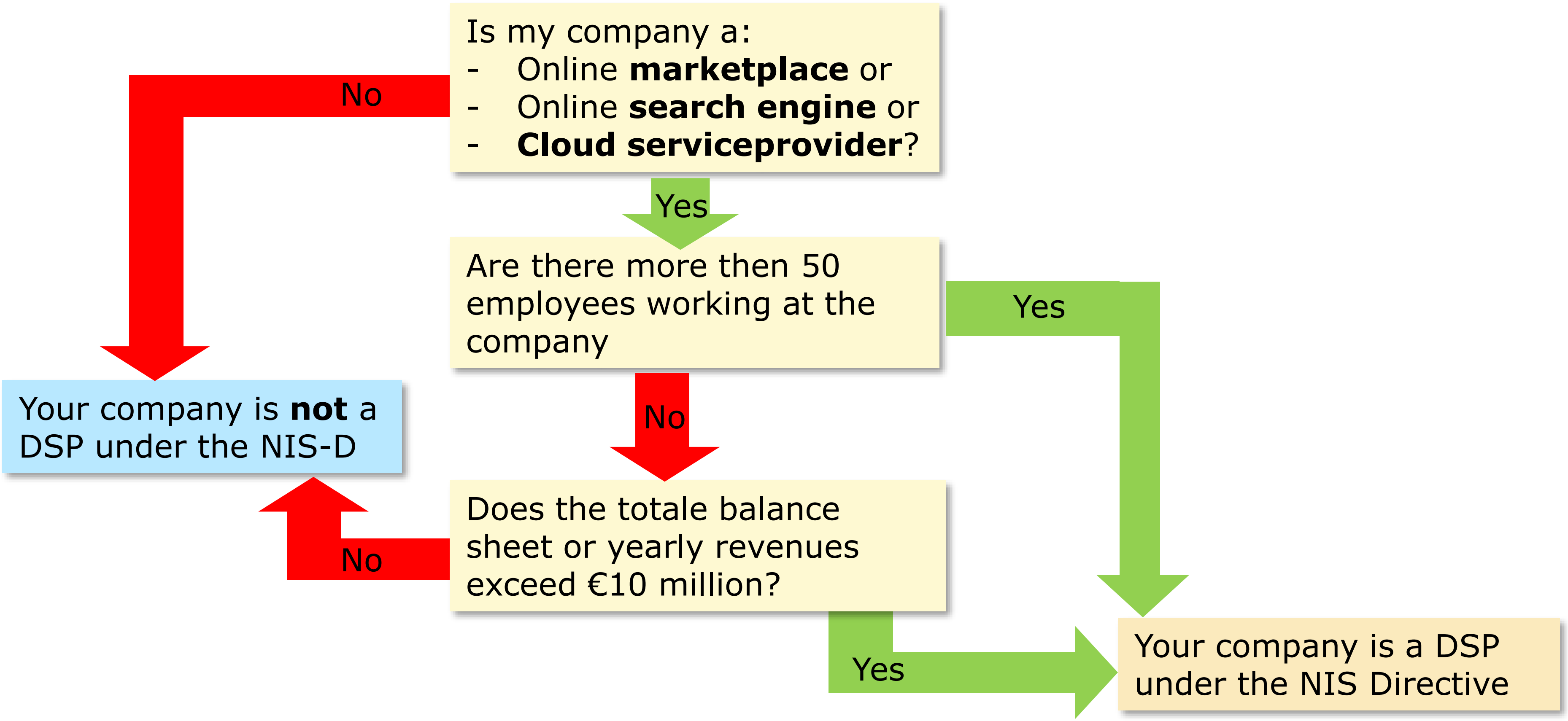
3. Cloud computing services

- allow access to a scalable and elastic pool of shareable computing resources.
- Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services.

- SAAS, PAAS, IAAS

4. Exception Small and Micro Enterprises

Is your company a DSP under NIS-D?



Is my company a:
- Online **marketplace** or
- Online **search engine** or
- **Cloud serviceprovider**?

No

Yes

Are there more then 50 employees working at the company

Yes

No

Your company is **not** a DSP under the NIS-D

Does the totale balance sheet or yearly revenues exceed €10 million?

No

Yes

Your company is a DSP under the NIS Directive

If your company is owned >25% by an other company then numbers should be accumulated.

Consequences

1. Security measures
2. Incident reporting
3. Competent authorities

1. Security measures

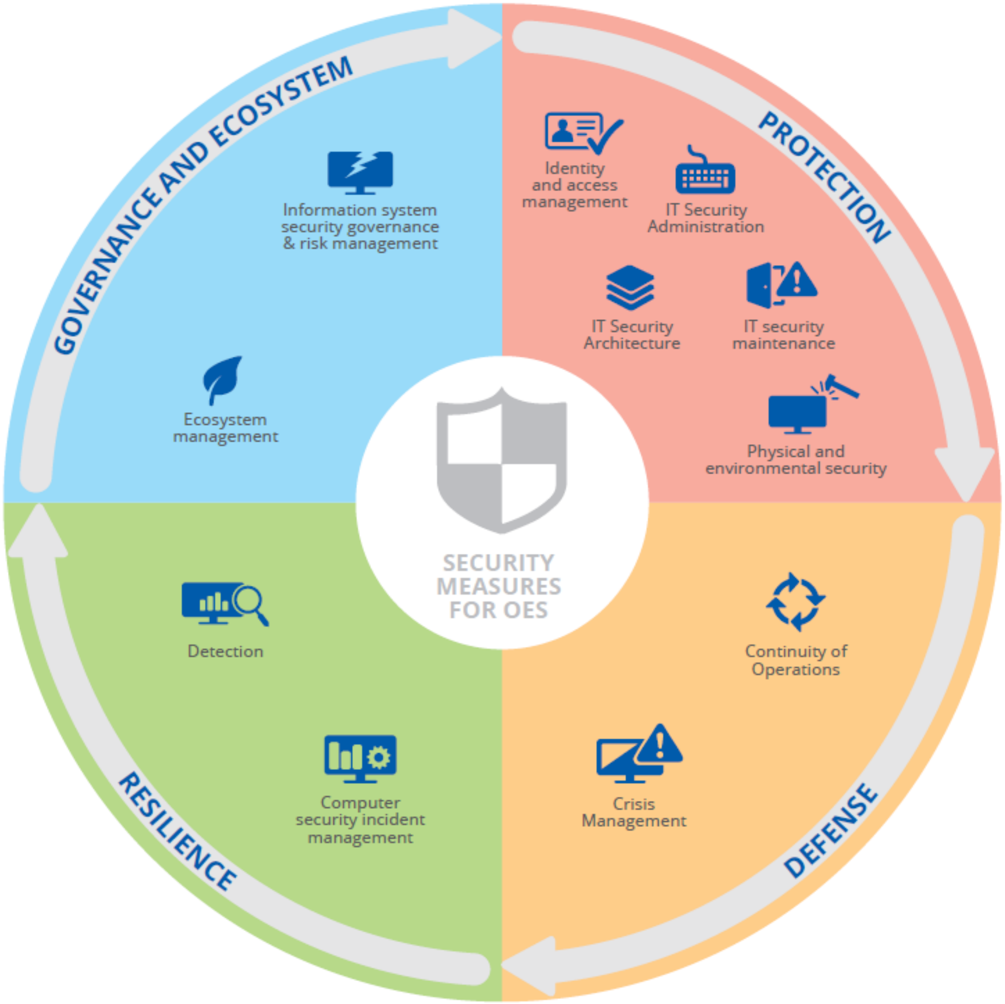
- “Digital Service Providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems”
- Measures include:
  a) the security of systems and facilities
  b) incident handling
  c) business continuity management
  d) monitoring, auditing and testing
  e) compliance with international standards

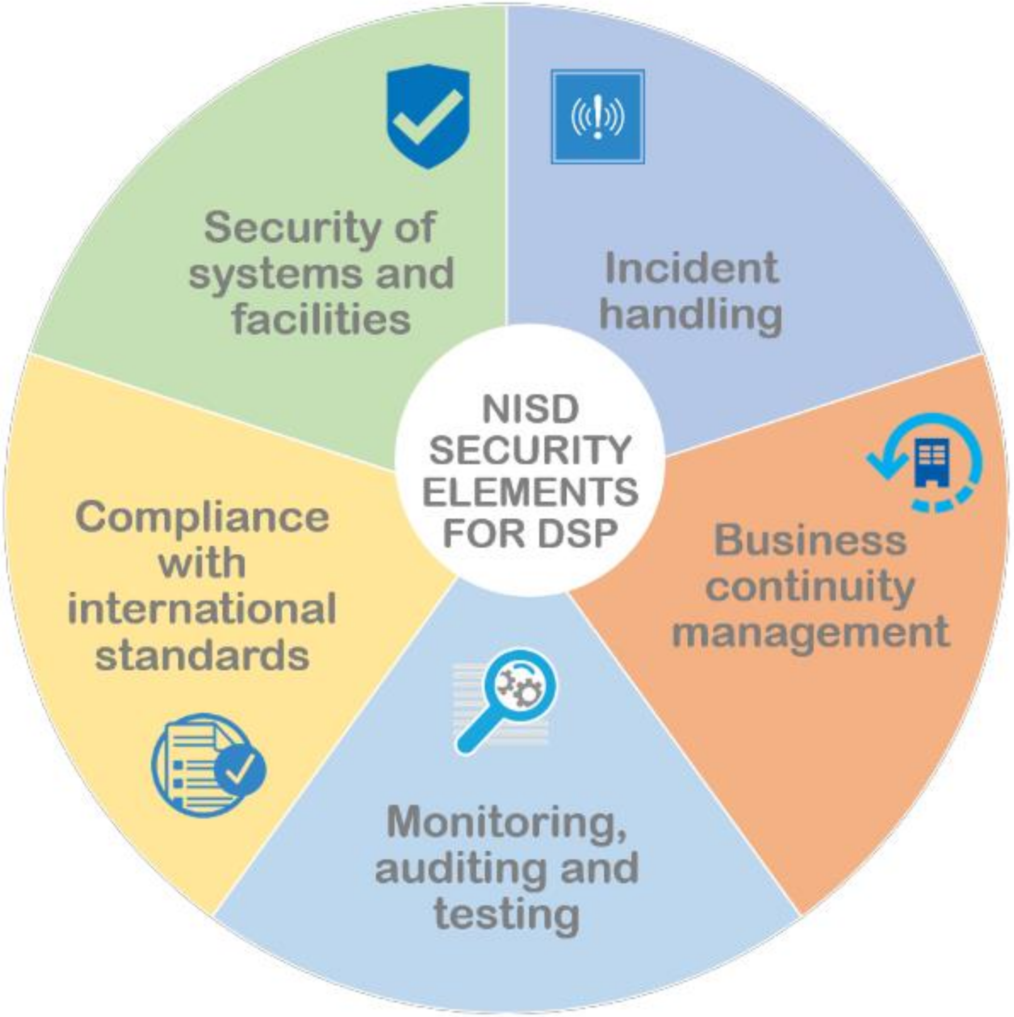
Risk Analysis

To identify risks and determine appropriate and proportionate:

- Perform systematic assessments and analysis
- Risk-based approach
- Identify specific risks and quantify their significance
- Including:
  - management of network and information systems
  - the physical and environmental security
  - the security of supplies
  - the access controls

ENISA guidelines


GOVERNANCE AND ECOSYSTEM
PROTECTION
DEFENSE
RESILIENCE
Information system security governance & risk management
Ecosystem management
Identity and access management
IT Security Administration
IT Security Architecture
IT security maintenance
Physical and environmental security
Continuity of Operations
Crisis Management
Computer security incident management
Detection
SECURITY MEASURES FOR OES


NISD SECURITY ELEMENTS FOR DSP
Security of systems and facilities
Incident handling
Business continuity management
Monitoring, auditing and testing
Compliance with international standards

https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

2. Incident reporting

- Substantial incidents must be reported
- In the Member State of the main establishment

- Incidents are at least substantial in case
  - Service unavailable more then 5 million user hours
  - Affecting more than 100 000 users
  - Created a risk to public safety, public security or of loss of life
  - Damage to at least one user of over €1.000.000

3. Competent Authorities

- Supervision is reactive (not pro active)
- Based on incident reporting of other signals
- DSP’s need to proof that they are compliant

Incident reporting in Italy

- Ministry of Economic Development –
  High Institute for communications and information technology (ISCTI)

- Incidents must be reported to: notifica.nis@csirt-ita.it

- More information: https://www.csirt-ita.it/

Questions

NIS Directive:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Implementation Regulation DSP's:
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32018R0151

Huub Janssen

huub.janssen@agentschaptelecom.nl

+31629044045

Discussion

1. Opportunities and threats

2. Impact of NIS on
   - Fintech?
   - Smart mobility?
   - Smart city?
   - eHealth?